

# 用户手册

## TL-R1660M

## 多功能宽带路由器

*选择知名品牌*

*品质更有保障*

Rev. 1.0
71035645



**深圳市普联技术有限公司**
**TP-LINK TECHNOLOGIES CO., LTD.**
技术支持热线：0755-26617951
技术支持E-mail：fae@tp-link.com.cn
网址：http://www.tp-link.com.cn
地址：深圳市南山区西丽镇红花岭工业区二区7栋

## 商标、版权声明

TP-LINK® 为深圳市普联技术有限公司的注册商标。本产品的所有组成部分，包括配件和软件在内，其版权都归深圳市普联技术有限公司所有，未经深圳市普联技术有限公司许可，不得任意仿制、拷贝、誊抄或转译。本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知，可随时查阅我们的万维网页http:// www.tp-link.com.cn。



# 目　　录

# 物 品 清 单

小心打开包装盒，检查包装盒里面应有以下配件：

- 一台路由器
- 一个电源
- 一本用户手册
- 一张保修卡

如果发现有所损坏或者任何配件短缺的情况，请及时和当地经销商联系。

# 第一章　用户手册简介

感谢您购买TL-R1660M多功能宽带路由器！TL-R1660M多功能宽带路由器是专为满足小型企业办公上网需要而设计的。允许多台计算机共享1条单独宽带线路和一个ISP账号。TL-R1660M功能齐全、性能优越、配置方便、使用简单，是您上网冲浪的最佳选择。

TL-R1660M多功能宽带路由器容易配置，无需专业人员即可按照本手册安装配置完成。在您准备安装使用产品之前，请先仔细阅读本手册，以全面利用产品的所有功能。

## 1.1　用　途

本手册的目的是帮助您熟悉和正确使用TL-R1660M多功能宽带路由器。

## 1.2　约　定

在本手册中所提到的路由器，如无特别说明，系指TL-R1660M多功能宽带路由器。

## 1.3　用户手册概述

第一章：用户手册简介。

第二章：产品概述。简述路由器的主要特性和规格。

第三章：硬件安装。帮助您进行路由器的硬件安装。

第四章：快速安装指南。帮助您配置路由器的基本网络参数。

第五章： 配置指南。帮助您配置路由器的高级特性。

附录A： 常见问题解答。

附录B： TCP/IP的详细配置。

附录C： 术语解释。







# 第二章　产品概述

## 2.1　产品简介

TL-R1660M 多功能宽带路由器是专为满足小型企业办公上网需要而设计的，性能优越、配置简单。此款路由器提供多方面的管理功能，可对系统、DHCP服务器、虚拟服务器、DMZ主机、防火墙、静态路由表等进行管理。

TL-R1660M 路由器可以限制对网站的浏览，以确保员工在许可的时间段内浏览指定的网站，杜绝浏览不良网站，可以有针对地开放指定计算机的上网权限，以便对部分人员的上网时段和浏览网站进行限制，而同时保障另一部分人员享有更多上网权限甚至不受限制。

TL-R1660M 路由器具有定时开启和关闭上网功能，可以在预先设定的时间内自动开通上网功能，减少网管人员工作。

TL-R1660M路由器可以根据上网动作自动连通和断开上网连接，在网络开通期间，如无人进行联网，路由器能自动断开连接，从而节省无谓的上网支出；当有人连接时，路由器能够自动开通网络恢复连接，省钱又省心。

TL-R1660M路由器具有全中文配置界面，配置简单，易于操作。快速配置向导更使您轻松实现网络连接和管理。在您操作的每一步，都有清晰详细的“帮助”说明，使您轻松掌握繁杂的网络配置。

## 2.2　特性和规格说明

### 2.2.1　主要特性

- 符合IEEE 802.3、IEEE 802.3u标准
- 支持TCP/IP、PPPoE、DHCP、ICMP、NAT、SNTP协议
- 提供1个10/100M自适应以太网（WAN）接口，可接xDSL/以太网/Cable

- 提供15个10/100M自适应以太网（LAN）接口
- 支持端口自动翻转（Auto MDI/MDIX）
- 内建DHCP服务器，同时可进行静态地址分配
- 内建防火墙，支持域名过滤和MAC地址过滤
- 支持静态路由
- 支持VPN Pass-through
- 支持虚拟服务器、DMZ主机
- 可防止DoS攻击，具有病毒自动隔离功能
- 支持IEEE 802.1X认证，内置IEEE 802.1X客户端，完全满足特殊运营商认证计费要求
- 支持通用即插即用（UPnP），符合UPnP标准的数据可顺利通过
- 支持动态DNS功能
- 可以有针对地开放指定计算机的上网权限
- 具有按需拨号和定时开启/关闭上网功能
- 支持MAC地址修改与克隆
- 提供系统安全日志、流量统计
- 支持远程和Web管理，全中文配置界面，配备简易安装向导（Wizard）
- 提供手动复位按钮
- 外置电源适配器，结构美观大方

### 2.2.2 规 格

- 符合IEEE 802.3 Ethernet以及IEEE 802.3u Fast Ethernet 标准
- 支持TCP/IP、PPPoE、DHCP、ICMP、NAT协议
- 流控方式：全双工采用IEEE 802.3x 标准，半双工采用Backpressure标准
- 端口支持自动协商功能，自动调整传输方式和传输速度
- 端口支持Auto MDI/MDIX自动翻转
- 提供状态指示灯，外置电源（电源输出9V～ 50Hz 1.2A）





# 第三章 硬件安装

## 3.1 面板布置

### 3.1.1 前面板

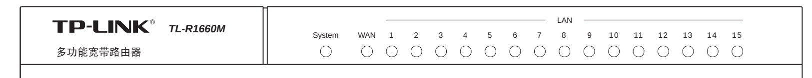



图3.1 TL-R1660M前面板示意图

指示灯：

| 指示灯 | 动 作 | 描 述 |
|---|---|---|
| System | 常灭/常亮 | 存在故障 |
| | 闪烁 | 工作正常 |
| WAN | 常灭 | 端口未连接设备 |
| | 常亮 | 端口已正常连接设备 |
| | 闪烁 | 端口正在收发数据 |
| LAN(1-15) | 常灭 | 端口未连接设备 |
| | 常亮 | 端口已正常连接设备 |
| | 闪烁 | 端口正在收发数据 |

### 3.1.2 后面板

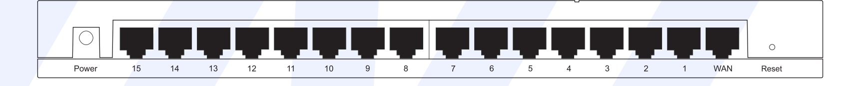



图3.2 TL-R1660M后面板示意图

1) **电源插孔**：这个插孔供您接插电源。注意：电源规格为9V～ 50Hz 1.2A，如果使用不匹配的电源，可能会导致路由器损坏。
2) Reset：复位按钮。断开电源并按住此按钮，连接电源，约过5秒钟，观察到System指示灯闪烁后，松开Reset复位按钮，系统配置将恢复到默认值。

**注　意：**

在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

3) WAN：1个广域网端口(RJ45)。连接xDSL Modem/Cable Modem或以太网。

4) **局域网端口：**15个RJ45接口（1~15）。计算机和集线器/交换机通过这些端口连入局域网。

## 3.2 系统需求

- 宽带Internet服务(接入方式为xDSL Modem/Cable Modem或以太网)
- 具有RJ45口的调制解调器（直接接入以太网不需要此设备）
- 每台PC的以太网连接（网卡和网线）
- TCP/IP网络软件（Windows 95/98/ME/NT/2000/XP自带）
- Internet Explorer 5.0 或更高版本

## 3.3 安装环境

**安装环境要求：**

- 将路由器水平放置。
- 放置路由器时请尽量远离发热器件。
- 不要将路由器置于太脏或潮湿的地方。

**路由器推荐使用环境：**

- 工作温度：0℃～40℃
- 存储温度：-40℃～70℃
- 工作湿度：10%～90%RH 不凝结
- 存储湿度：5%～90%RH 不凝结







## 3.4 硬件安装步骤

在安装路由器前，我们希望您已经能够利用您的宽带服务在单台计算机上成功上网。如果您单台计算机上网有问题，请先和您的网络提供商（ISP）联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装您的路由器。切记安装时拔除电源插头，保持双手干燥。

1) **建立局域网连接**

用一根网线连接路由器的1-15任一口和局域网中的集线器或交换机，如图3.3所示。您也可以用一根网线将路由器的1-15任一口与您的计算机网卡直接相连。

2) **建立广域网连接**

用一根网线连接路由器WAN口和xDSL Modem/Cable Modem或以太网，如下图所示。

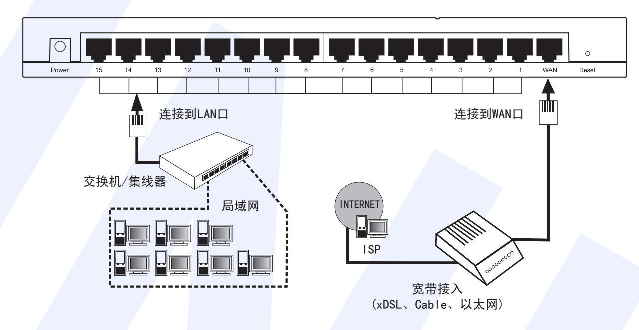



图3.3　建立局域网和广域网连接

3) **连接电源**

将电源连接好，路由器将自行启动。

# 第四章　快速安装指南

要正确使用路由器，您必须合理配置网络以及在您的计算机上安装软件（本用户手册以Windows 2000/XP为例）。如果进行基本配置，您只需阅读本章内容；如果进行高级配置，请继续阅读第五章内容。

## 4.1　建立正确的网络设置

路由器默认IP地址是192.168.1.1，默认子网掩码是255.255.255.0。这些值可以根据您的需要而改变，但是我们在这本用户手册上将按默认值说明。

首先请将您的计算机接到路由器的1～15口，接下来您可以使用两种方法为您的计算机设置IP地址。（详细设置请参考附录B）

**方法一、手动设置IP地址。**
设置您计算机的IP地址为192.168.1.xxx（xxx范围是2至254），子网掩码为255.255.255.0，默认网关为192.168.1.1，DNS服务器为192.168.1.1。

**方法二、利用路由器内置DHCP服务器自动设置IP地址。**
设置您计算机的TCP/IP协议为“自动获取IP地址”。

在设置好TCP/IP协议后，您可以使用Ping命令检查您的计算机和路由器之间是否联通。下面的例子为在Windows 2000环境中，执行Ping命令：按开始→运行→在命令框中输入cmd，然后按回车键，在出现的界面里输入：

Ping 192.168.1.1。如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```







那么恭喜您！您的计算机已与路由器成功建立连接。如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，您可以按照下列顺序检查：

1)　硬件连接是否正确？

**提　示：**
路由器面板上与您接入端口相对应的指示灯和您计算机上的网卡灯必须亮。

2)　您的计算机的TCP/IP设置是否正确？

**提　示：**
如果路由器的IP地址为192.168.1.1, 那么您的计算机IP地址必须为192.168. 1.xxx（xxx范围是2~254），而且默认网关为192.168. 1.1。

## 4.2　快速安装指南

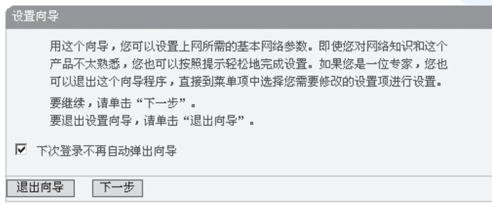
本产品提供基于浏览器（Internet Explorer或Netscape Communicator）的配置界面，这种配置方案适宜于任何MS Windows，Macintosh或UNIX平台。

激活浏览器，取消“使用代理服务器”选项或者将路由器的IP地址添加到“代理服务器设置”中的“例外”栏中（在IE中选择“工具—Internet选项—连接—局域网设置”，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的IP地址，例如 http://192.168.1.1。

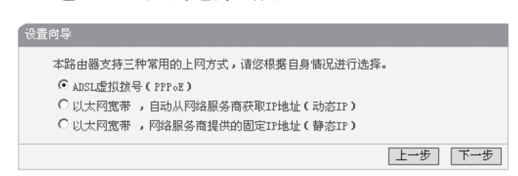
连接建立起来后，您将会看到下图所示登录界面。在该登录界面输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。




如果名称和密码正确，浏览器将显示管理员模式的画面，并会弹出一个设置向导的画面（如果没有自动弹出的话，可以单击管理员模式画面左边“设置向导”菜单将它激活）。如果这里连续多次输入错误，则会进入到一个显示错误的界面。




单击“下一步”，进入上网方式选择画面。



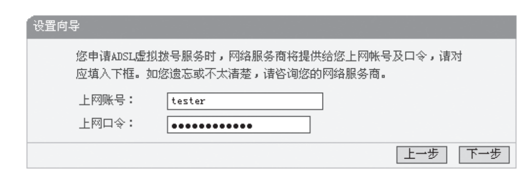

以上画面显示了最常用的三种上网方式，您可以根据自身情况进行选择，然后单击“下一步”填写上网所需的基本网络参数。

1) 如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，则您需要填写以下内容：（填写时不清楚的项目请向ISP询问）





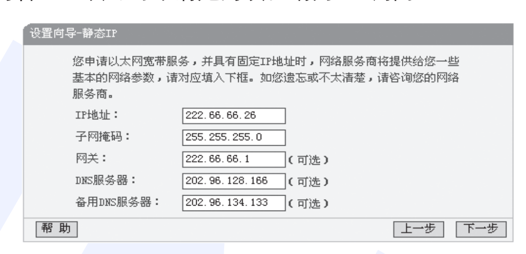





- 上网账号：填入ISP为您指定的ADSL上网账号。
- 上网口令：填入ISP为您指定的ADSL上网口令。

2) 如果您的上网方式为动态IP，即您可以自动从ISP获取IP地址，则无需填写参数。

3) 如果您的上网方式为静态IP，即您拥有ISP提供的固定IP地址，则您需要填写以下内容：（填写时不清楚的项目请向ISP询问）




- IP地址：本路由器对广域网的IP地址，即ISP提供给您的IP地址。
- 子网掩码：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
- 网关：填入ISP提供给您的网关。
- DNS服务器：填入ISP提供给您的DNS服务器地址。
- 备用DNS服务器：可选项，如果ISP提供给您了两个DNS服务器地址，则您可以把另一个DNS服务器的IP地址填于此处。

在设置完上网所需的各项网络参数后，您即可看到设置向导完成画面。

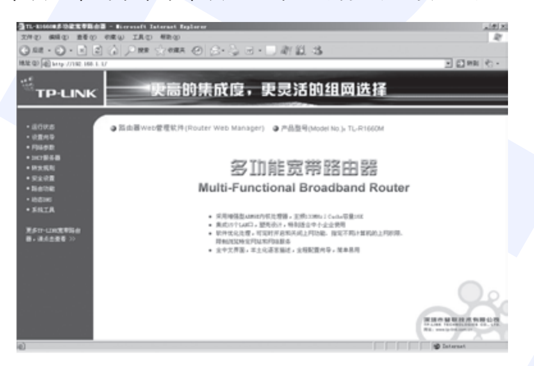


# 第五章　配置指南

## 5.1　启动和登录

启动路由器并登录成功后，浏览器会显示管理员模式的画面。

在左侧菜单栏中，共有“运行状态”、“设置向导”、“网络参数”、“DHCP服务器”、“转发规则”、“安全设置”、“路由功能”、“动态DNS”和“系统工具”等菜单项。单击某个菜单项，您即可进行相应的功能设置。




下面将详细讲解各个菜单的功能。





## 5.2　运行状态



版本信息

| | |
|---|---|
| 当前软件版本： | 3.4.0 Build 061209 Rel.34233na |
| 当前硬件版本： | R1660M v1 1001225B |

LAN口状态

| | |
|---|---|
| MAC 地址： | 00-0A-EB-00-13-01 |
| IP地址： | 192.168.1.1 |
| 子网掩码： | 255.255.255.0 |

WAN口状态

| | | |
|---|---|---|
| MAC 地址： | 00-0A-EB-00-13-02 | |
| IP地址： | 222.66.66.26 | 静态IP |
| 子网掩码： | 255.255.255.0 | |
| 网关： | 222.66.66.1 | |
| DNS 服务器： | 202.96.134.133 , 202.96.128.166 | |

WAN口流量统计

| | 接收 | 发送 |
|---|---|---|
| 字节数： | 0 | 0 |
| 数据包数： | 0 | 0 |

| | | |
|---|---|---|
| 运行时间： | 0 day(s) 00:07:53 | 刷 新 |

本页显示路由器工作状态。

1)　版本信息

此处显示路由器当前软硬件的版本号。

2)　LAN口状态

此处显示当前LAN口的MAC地址、IP地址和子网掩码。

3)　WAN口状态

此处显示当前WAN口的MAC地址、IP地址、子网掩码、网关和DNS服务器地址。同时右侧将显示用户上网方式（PPPoE/动态IP/静态IP）。如果用户的上网方式为PPPoE、L2TP、PPTP（ADSL拨号上网），当用户已经连接Internet时，此处将会显示用户的上网时间和“断线”按钮，单击此按钮可以进行即时的断线操作，当用户尚未连接Internet时，此处将会显示“连接”按钮，单击此按钮可以进行即时的连接操作。

4)　WAN口流量统计

此处显示当前WAN口接收和发送的数据流量信息。

## 5.3 设置向导

请参考第四章的快速安装指南。

## 5.4 网络参数

- 网络参数
  - LAN口设置
  - WAN口设置
  - MAC地址克隆

在“网络参数”菜单下面，共有“LAN口设置”、“WAN口设置”和“MAC地址克隆”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

### 5.4.1 LAN口设置




本页设置LAN口的基本网络参数。

- MAC地址：本路由器对局域网的MAC地址，此值不可更改。
- IP地址：本路由器对局域网的IP地址。该IP地址出厂设置为192.168.1.1，您可以根据需要改变它。





**注　意：**

如果您改变了本IP地址，您必须用新的IP地址才能登录路由器进行WEB界面管理，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。

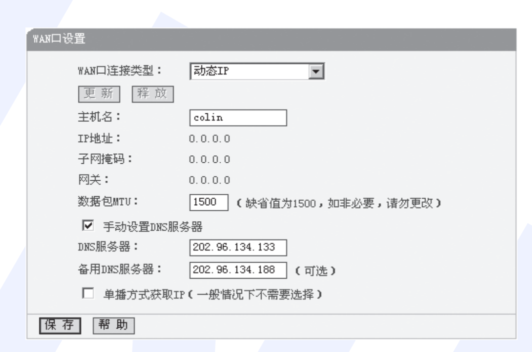
- 子网掩码：本路由器对局域网的子网掩码，可以在下拉列表中选择B类（255.255.0.0）或者C类（255.255.255.0）地址的子网掩码。一般情况下选择255.255.255.0即可。



**注　意：**

局域网中所有计算机的子网掩码必须与此处设置相同。

### 5.4.2 WAN口设置




首先请您选择您的WAN口连接类型，即您的上网方式。本路由器默认上网方式为“动态IP”。

1) 如果您的选择是“动态IP”，即路由器可以自动从ISP获取IP地址，您将会看到如上图所示页面。

该页面将显示您从ISP的DHCP服务器动态得到的IP地址、子网掩码、网关、DNS服务器等信息。你可以单击“更新”按钮，从ISP的DHCP服务器更新

WAN口的IP地址、子网掩码、网关、DNS服务器等设置。您也可以单击“释放”按钮，发送DHCP释放请求到ISP的DHCP服务器，释放IP设置。如果您想手动设置自己的DNS服务器的话，亦可在此处进行相应设置。少数ISP的DHCP服务器不支持广播的请求方式，如果您在网络连接正常的情况下无法获取IP地址，可以尝试选择“单播方式获取IP”。

➢ 数据包MTU：填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。

2) 如果您的选择是“静态IP”，即您拥有ISP提供的固定IP地址，您将会看到如下图所示页面，在该页面您需要设置以下项目：（填写时不清楚的项目请向ISP询问）

WAN口设置

WAN口连接类型：静态IP
IP地址：222.66.66.26
子网掩码：255.255.255.0
网关：222.66.66.1（可选）
数据包MTU：1500（缺省值为1500，如非必要，请勿更改）
DNS服务器：202.96.128.166（可选）
备用DNS服务器：202.96.134.133（可选）
保 存　帮 助

➢ IP地址：本路由器对广域网的IP地址，即ISP提供给您的IP地址。
➢ 子网掩码：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
➢ 网关：填入ISP提供给您的网关。
➢ 数据包MTU：填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。
➢ DNS服务器：填入ISP提供给您的DNS服务器地址。
➢ 备用DNS服务器：可选项，如果ISP提供给您了两个DNS服务器地址，则您可以把另一个DNS服务器的IP地址填于此处。

3) 如果您的选择是“PPPoE”，即您的上网的方式为ADSL虚拟拨号方式，





您将会看到如下图所示页面，在该页面您需要设置以下项目：（填写时不清楚的项目请向ISP询问）



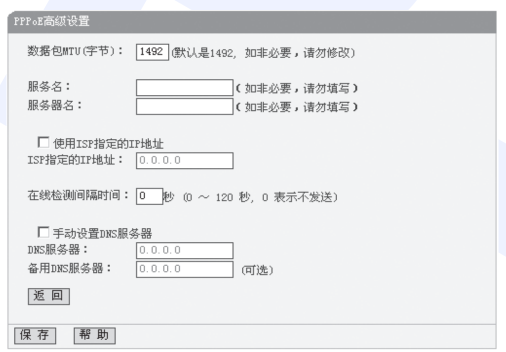

➢ 上网账号：填入ISP为您指定的ADSL上网账号。
➢ 上网口令：填入ISP为您指定的ADSL上网口令。
➢ 按需连接：如果选择了按需连接，则在有来自局域网的网络访问请求时，自动进行连接操作。
➢ 自动断线等待时间：如果自动断线等待时间T不等于0（默认时间为15分钟），则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
➢ 自动连接：如果选择了自动连接，则在开机后自动进行连接操作。在使用过程中，如果由于外部原因，网络被断开，则每隔一段时间（30秒）尝试进行连接，直到连接上为止。
➢ 定时连接：如果选择了定时连接，则在“连接时段”指定起始时间自动进行连接操作，在指定终止时间自动进行断线操作。

**注　意：**

只有当您到“系统工具”的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。

- 手动连接：开机后由用户手动进行ADSL拨号连接。
- 连接/断开：单击此按钮，进行即时的连接/断开操作。

您还可以根据实际需要，进入到“高级设置”界面对相关设置项进行设置、调整。




- 数据包MTU：填入网络数据包的MTU值，缺省为1492，如非特别需要，一般不要更改。
- 服务名：Service Name，如果不是ISP特别要求，请不要填写。
- 服务器名称：AC Name，如果不是ISP特别要求，请不要填写。
- 使用ISP指定IP地址：如果您的ISP为您指定了IP地址，请选中此选择框，并在“ISP指定的IP地址”栏后填入ISP为您指定的IP地址。
- 在线检测时间间隔： 路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送。
- DNS服务器：从ISP处自动获得的DNS服务器地址，或者您可以在此处手动设置自己的DNS服务器地址。
- 备用DNS服务器：从ISP处自动获得的备用DNS服务器地址，或者您可以





在此处手动设置自己的备用DNS服务器地址。

4) IEEE 802.1X＋动态IP

如果您选择的是“IEEE 802.1X+动态IP”，即您可以自动从ISP获取IP地址，但是您首先要先进行802.1X认证，否则将无法获得IP地址或者连通外网。设置界面如下图所示：




首先您需要设置“用户名”和“密码”，这是进行802.1X认证所必需的。当您点击“登录”按钮，并且界面显示“登录成功！”之后，您就可以点击“更新”按钮，从ISP的DHCP服务器更新WAN口的IP地址、子网掩码、网关、DNS服务器等设置。

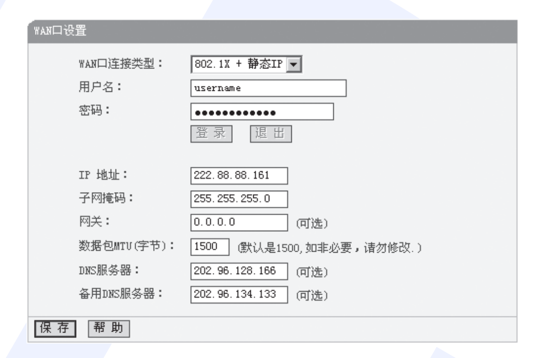
您也可以单击“释放”按钮，发送DHCP释放请求到ISP的DHCP服务器，释放IP设置。少数ISP的DHCP服务器不支持广播方式的请求方式，您在网络连接正常的情况下无法获得IP地址，可以尝试选择“单播方式获取IP”。

- 数据包MTU：填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。

5) IEEE 802.1X+静态IP

如果您选择的是“IEEE 802.1X+静态IP”，即您拥有ISP提供的固定IP地址，

但是您首先要先进行802.1X认证，否则将无法连通Internet。设置界面如下图所示，在该页面您需要设置以下项目：（填写时不清楚的项目请向ISP询问）




- 用户名：ISP提供的 802.1X 的用户名。
- 密码：ISP提供的 802.1X 的密码。
- IP地址：本路由器对广域网的IP地址，即ISP提供给您的IP地址。
- 子网掩码：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
- 网关：填入ISP提供给您的网关地址。
- 数据包MTU：填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。
- DNS服务器：填入ISP提供给您的DNS服务器地址。
- 备用DNS服务器：可选项，如果ISP提供给您了两个DNS服务器地址，则您可以把另一个DNS服务器的IP地址填于此处。

6) L2TP

如果您选择的是“L2TP”，您将会看到如下图所示页面，在该页面您需要设置以下项目：（填写时不清楚的项目请向ISP询问）








- 上网账号：填入ISP为您指定的上网账号。
- 上网口令：填入ISP为您指定的上网口令。
- 连接/断线：单击此按钮，进行即时的连接/断开操作。
- 动态IP：如果您可以自动从ISP获取IP地址，请选择“动态IP”。您将会通过ISP的DHCP服务器自动获得IP地址、子网掩码、网关和DNS服务器。
- 静态IP：如果您拥有ISP提供的固定IP地址，请选择“静态IP”。此时，您需要手动设置IP地址、子网掩码、网关和DNS服务器。
- 服务器IP/域名：填入ISP为您指定的IP或域名。
- IP地址：本路由器对广域网的IP地址，即ISP提供给您的IP地址。
- 子网掩码：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
- 网关：ISP提供给您的网关。
- DNS：ISP提供给您的DNS服务器地址。

- 数据包MTU：填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。
- 自动断线等待时间：如果自动断线等待时间T不等于0（默认时间为15分钟），则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 按需连接：如果选择了按需连接，则在有来自局域网的网络访问请求时，自动进行连接操作。
- 自动连接：如果选择了自动连接，则在开机后自动进行连接操作。在使用过程中，如果由于外部原因，网络被断开，则每隔一段时间（30秒）尝试进行连接，直到连接上为止。
- 手动连接：开机后由用户手动进行连接。

7) PPTP

如果您选择的是“PPTP”，您将会看到如下图所示页面，在该页面您需要设置以下项目：（填写时不清楚的项目请向ISP询问）

WAN口设置

WAN口连接类型： PPTP

上网帐号： user-colin

上网口令： ●●●●●

连 接　断 线　未连接

○ 动态 IP　◉ 静态 IP

服务器 IP /域名： 192.169.1.5

IP 地址： 192.169.1.26

子网掩码： 255.255.255.0

网关： 192.168.1.1

DNS： 0.0.0.0

Internet IP： 0.0.0.0

Internet DNS： 0.0.0.0 , 0.0.0.0

数据包MTU(字节)： 1460 （缺省值为1460，如非必要，请勿修改）

根据您的需要，请选择对应的连接模式：

自动断线等待时间： 15 分 (0 表示不自动断线)

◉ 按需连接，在有访问数据时自动进行连接

○ 自动连接，在开机和断线后自动连接

○ 手动连接，由用户手动连接

保 存　帮 助

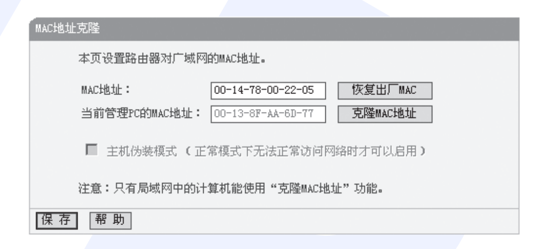






- 上网账号：填入ISP为您指定的上网账号。
- 上网口令：填入ISP为您指定的上网口令。
- 连接/断线：单击此按钮，进行即时的连接/断开操作。
- 动态IP：如果您可以自动从ISP获取IP地址，请选择“动态IP”。您将会通过ISP的DHCP服务器自动获得IP地址、子网掩码、网关和DNS服务器。
- 静态IP：如果您拥有ISP提供的固定IP地址，请选择“静态IP”。此时，您需要手动设置IP地址、子网掩码、网关和DNS服务器。
- 服务器IP/域名：填入ISP为您指定的IP或域名。
- IP地址：本路由器对广域网的IP地址，即ISP提供给您的IP地址。
- 子网掩码：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
- 网关：ISP提供给您的网关。
- DNS：ISP提供给您的DNS服务器地址。
- 数据包MTU：填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。
- 自动断线等待时间：如果自动断线等待时间T不等于0（默认时间为15分钟），则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 按需连接：如果选择了按需连接，则在有来自局域网的网络访问请求时，自动进行连接操作。
- 自动连接：如果选择了自动连接，则在开机后自动进行连接操作。在使用过程中，如果由于外部原因，网络被断开，则每隔一段时间（30秒）尝试进行连接，直到连接上为止。
- 手动连接：开机后由用户手动进行连接。

### 5.4.3 MAC地址克隆




本页设置路由器对广域网的MAC地址。

- MAC地址：本路由器对广域网的MAC地址，此值一般不用更改。但某些ISP可能会要求对MAC地址进行绑定，此时ISP会提供一个有效的MAC地址给用户，您只要根据它所提供的值，输入到“MAC地址”栏，然后单击“保存”，您即可改变本路由器对广域网的MAC地址。
- 当前管理PC的MAC地址：当前正在进行管理操作的计算机的MAC地址。
- 恢复出厂MAC：单击此按钮，您即可恢复本路由器对广域网的MAC地址为出厂时的默认设置。
- 克隆MAC地址：单击此按钮，您即可把当前管理PC的MAC地址克隆到“MAC地址”栏内。

 **注　意：**

只有局域网中的计算机能使用“克隆MAC地址”功能。按“保存”按钮后，路由器将自动重启。

## 5.5 DHCP服务器

- DHCP服务器
  - DHCP服务
  - 客户端列表
  - 静态地址分配



TL-R1660M 多功能宽带路由器用户手册
5. 配置指南

在“DHCP服务器”菜单下面，有“DHCP服务”、“客户端列表”和“静态地址分配”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

### 5.5.1 DHCP服务

DHCP服务

本路由器内建DHCP服务器，它能自动替您配置局域网中各计算机的TCP/IP协议。

DHCP服务器：○不启用 ◉启用
地址池开始地址：192.168.1.100
地址池结束地址：192.168.1.199
地址租期：120 分钟（1～2880分钟，缺省为120分钟）
网关：0.0.0.0（可选）
缺省域名：（可选）
主DNS服务器：0.0.0.0（可选）
备用DNS服务器：0.0.0.0（可选）
保 存　帮 助

TCP/IP协议设置包括IP地址、子网掩码、网关、以及DNS服务器等。为您局域网中所有的计算机正确配置TCP/IP协议并不是一件容易的事，幸运的是，DHCP服务器提供了这种功能。如果您使用本路由器的DHCP服务器功能的话，您可以让DHCP服务器自动替您配置局域网中各计算机的TCP/IP协议。

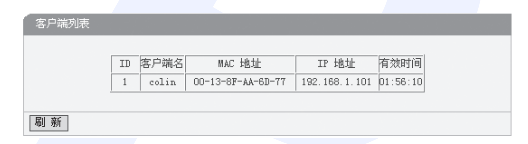
要使用DHCP服务器功能，您需要设置以下项目：

- 地址池开始地址：DHCP服务器所自动分配的IP的起始地址。
- 地址池结束地址：DHCP服务器自动分配的IP的结束地址。
- 网关：填入路由器LAN口的IP地址，缺省是192.168.1.1。
- 缺省域名：可选项，填入本地网域名（默认为空）。
- 主DNS服务器：可选项，填入ISP提供给您的DNS服务器地址，不清楚可以向ISP询问。
- 备用DNS服务器：可选项，如果ISP提供给您了两个DNS服务器地址，则您可以把另一个DNS服务器的IP地址填于此处。

**注　意：**

为了使用本路由器的DHCP服务器功能，局域网中计算机的TCP/IP协议必须设置为“自动获得IP地址”。此功能需要重启路由器才生效。

### 5.5.2 客户端列表




| ID | 客户端名 | MAC 地址 | IP 地址 | 有效时间 |
|---|---|---|---|---|
| 1 | colin | 00-13-8F-AA-6D-77 | 192.168.1.101 | 01:56:10 |

客户端列表罗列出所有通过DHCP获得IP的主机的信息：

- 客户端名：客户端计算机的名称。
- MAC地址：客户端计算机的MAC地址。
- IP地址：DHCP服务器分配给客户的IP地址。
- 有效时间：主机通过DHCP获得IP后离到期的时间，客户端软件会在租期到期前自动续约。

### 5.5.3 静态地址分配




| ID | MAC地址 | IP地址 | 状 态 | 配 置 |
|---|---|---|---|---|
| 1 | 00-13-8F-AA-6D-77 | 192.168.1.155 | 生效 | 编辑 删除 |

为了方便您对局域网中计算机的IP地址进行控制，本路由器内置了静态地址分配功能。静态地址分配表可以为具有指定MAC地址的计算机预留静态的IP地址。之后，此计算机请求DHCP服务器获得IP地址时，DHCP服务器将给它分配预留的IP地址。

- MAC地址：欲预留IP地址的计算机的MAC地址。

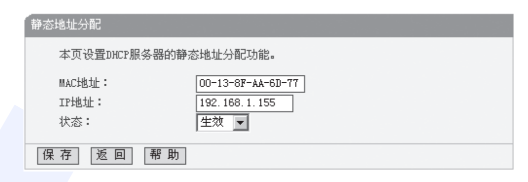


TL-R1660M 多功能宽带路由器用户手册

5. 配置指南

- IP地址：预留的IP地址。
- 状态：该条目是否生效。
- 配置：可对该条目进行的操作。
- 添加新条目：可通过该按钮增加新静态地址的条目。
- 使所有条目生效：该按钮使所有静态条目生效。
- 使所有条目失效：该按钮使所有静态条目失效。
- 删除所有条目：该按钮删除当前所有静态条目。

以下是点击“添加新条目”时的页面：

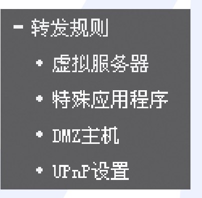





**注　意：**

此功能需要重启路由器才生效。

## 5.6 转发规则




在“转发规则”菜单下面，有“虚拟服务器”、“特殊应用程序” 、“DMZ主机”和“UPnP设置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

### 5.6.1 虚拟服务器

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

| ID | 服务端口 | IP地址 | 协议 | 状态 | 配置 |
|---|---|---|---|---|---|
| 1 | 21 | 192.168.1.2 | ALL | 生效 | 编辑 删除 |
| 2 | 80 | 192.168.1.3 | ALL | 生效 | 编辑 删除 |
| 3 | 110 | 192.168.1.6 | ALL | 生效 | 编辑 删除 |

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

本路由器自身集成了防火墙，这样广域网中的计算机要想通过本路由器访问局域网中的某些服务器，则在默认设置下无法通过防火墙的防护，这就出现了一对矛盾，路由器既要保护网络不被侵袭，又要方便广域网合法的用户访问。这里，本路由器提供了虚拟服务器功能，即可以解决这一对矛盾。虚拟服务器定义一个服务端口，所有对此端口的服务请求将被重新定位给通过IP地址指定的局域网中的服务器。

- 服务端口号：路由器提供给广域网的服务端口。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。
- IP地址：局域网中作为服务器的计算机的IP地址。
- 协议：选择协议数据包的类型,可供选择的有：TCP、UDP和ALL。
- 状态：只有选中生效后本条目所设置的规则才能生效。
- 添加新条目：添加新的虚拟服务器条目。
- 使所有条目生效：使所有虚拟服务器条目生效。
- 使所有条目失效：使所有虚拟服务器条目失效。
- 删除所有条目：删除所有虚拟服务器条目。

以下是你点击添加新条目时的页面：





虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号： 21 (XX-XX or XX)
IP地址： 192.168.1.2
协议： ALL
状态： 生效
常用服务端口号： --请选择--

保 存 返 回 帮 助

在“常用服务端口”中，列出了常用的协议的端口，您可以直接在其中选中一个，对于常用服务端口中没有列出的端口，您也可以在服务端口号处手动添加。

设置好以后，只要您在局域网的服务器上进行相应的设置，广域网的计算机就可以访问到您局域网的服务器上了。

举例说明：如果您的FTP服务器（端口号为21）IP地址为192.168.1.2，Web服务器（端口号为80）地址为 192.168.1.3，POP3服务器（端口号为110）IP地址为 192.168.1.6，这时您需要指定如下的虚拟服务器映射表：

| ID | 服务端口 | IP地址 | 协议 | 状态 | 配置 |
|---|---|---|---|---|---|
| 1 | 21 | 192.168.1.2 | ALL | 生效 | 编辑 删除 |
| 2 | 80 | 192.168.1.3 | ALL | 生效 | 编辑 删除 |
| 3 | 110 | 192.168.1.6 | ALL | 生效 | 编辑 删除 |

**注　意：**

如果设置了服务端口为80的虚拟服务器，则需要将“安全设置”菜单中“远端WEB管理”项的WEB管理端口设置为80以外的值，如8080，否则会发生冲突，而导致虚拟服务器不起作用。

### 5.6.2 特殊应用程序



特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

| ID | 触发端口 | 触发协议 | 开放端口 | 开放协议 | 状态 | 配置 |
|---|---|---|---|---|---|---|
| 1 | 7175 | ALL | 51200-51201,51210 | ALL | 生效 | 编辑 删除 |

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

某些程序需要多条连接，如Internet网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的NAT路由器下工作，特殊应用程序使得某些这样的应用程序能够在NAT路由器下工作。当一个应用程序在触发端口上发起连接时，在开放端口中的所有端口就会打开，以备后续连接。

- ➢ 触发端口：该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放，否则开放端口中的所有端口是不会开放的。
- ➢ 触发协议：可以选择ALL、UDP和TCP，代表触发端口上使用的协议。
- ➢ 开放端口：当在触发端口上发起连接后，开放端口打开，应用程序可以在该开放端口上发起后续的连接。可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。
- ➢ 开放协议：可以选择ALL、UDP和TCP，代表开放端口上使用的协议。
- ➢ 状态：只有该项为生效状态本条目所设置的规则才能生效。
- ➢ 添加新条目：在列表中添加新的条目。
- ➢ 使所有条目生效：将该列表中所有条目的状态设为“生效”。
- ➢ 使所有条目失效：将该列表中所有条目的状态设为“失效”。
- ➢ 删除所有条目：删除当前已设的所有条目。

以下是你点击添加新条目时的页面：

特殊应用程序
某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。
触发端口： 7175
触发协议： ALL
开放端口： 51200-51201,51210
开放协议： ALL
状态： 生效
常用应用程序： --请选择--
保 存 返 回 帮 助

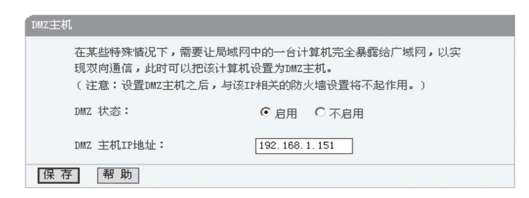






在“常用应用程序”中，列出了常用的应用程序，您可以直接在其中选中一个，对于常用应用程序中没有列出的程序，您也可以手动填写。

### 5.6.3 DMZ主机




在某些特殊情况下，我们需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。

设置步骤如下：首先在DMZ主机IP地址栏内输入欲设为DMZ主机的局域网计算机的IP地址，然后选中“启用”，最后单击“保存”完成DMZ主机的设置。

### 5.6.4 UPnP设置

依靠UPnP（Universal Plug and Play）协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP和Windows ME系统上安装的MSN Messenger在使用音频和视频通话时就可以利用UPnP协议，这样原本受限于NAT的功能可以恢复正常使用。

使用UPnP的方法如下：

1、 点击“启用UPnP”按钮开启UPnP功能。

2、 当MSN Messenger等程序在运行中使用本功能时，按“刷新”按钮可以看到端口转换信息。端口转换信息由应用程序发出请求时提供，各项目的含义如下：

- ➢ 应用描述：应用程序通过UPnP向路由器请求端口转换时给出的描述。
- ➢ 外部端口：端口转换使用的路由器端口号。

- 协议类型：表明是对TCP还是UDP进行端口转换。
- 内部端口：需要进行端口转换的主机端口号。
- IP地址：需要进行端口转换的主机IP地址。
- 状态：状态可以是“√”或“×”。“√”表示应用程序请求并启用了端口转换；“×”表示应用程序请求了端口转换但并没有启用。
- 删除：选取复选框，表示在点击“删除”按钮后，该条目将被删除。

3、 如果需要将某条目手工删除，请在删除栏选中该条目，再点击“删除”按钮，此时所有被选中的条目将被删除。

4、 如果希望将所有条目删除，请点击“删除所有”按钮，并确认即可。

5、 不使用时请点击“关闭UPnP”按钮关闭UPnP功能。

**注　意：**

1、 因为现阶段版本的UPnP协议的安全性还未得充分保证，在不需要时请关闭UPnP功能。

2、 只有支持UPnP协议的应用程序才能使用本功能，MSN Messenger 还可能需要操作系统的支持（如Windows XP/ME）。

3、 UPnP功能需要操作系统支持（如Windows XP/ME）。

## 5.7 安全设置

- 安全设置
  - 防火墙设置
  - IP地址过滤
  - 域名过滤
  - MAC地址过滤
  - 远端WEB管理
  - 高级安全设置

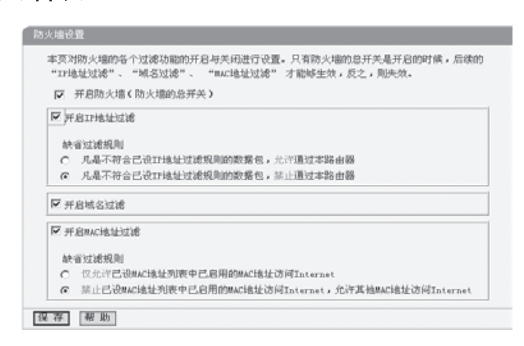
在“安全设置”菜单下面，共有“防火墙设置”、“IP地址过滤”、“域名过滤”、“MAC地址过滤”、“远端WEB管理”和“高级安全设置”六个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。







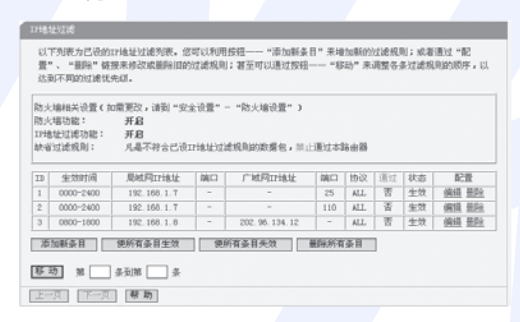
### 5.7.1 防火墙设置




本页对防火墙的各个过滤功能的开启与关闭进行设置。只有防火墙的总开关是开启的时候，后续的“IP地址过滤”、“域名过滤”、“MAC地址过滤”和“高级安全设置”才能够生效，反之，则失效。（建议在过滤规则设置完成后再开启防火墙总开关）

- 开启防火墙： 这是防火墙的总开关，当该开关关闭时，“IP地址过滤”、“域名过滤”、“MAC地址过滤”功能将全部失效。
- 开启IP地址过滤： 关闭或开启IP地址过滤功能。
- 开启域名过滤： 关闭或开启域名过滤功能。
- 开启MAC地址过滤： 关闭或开启MAC地址过滤功能。

### 5.7.2 IP地址过滤



本页显示已设的IP地址过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“修改”、“删除”链接来修改或删除旧的过滤规则；甚至可以通过按钮—“移动”来调整各条过滤规则的顺序，以达到不同的过滤优先级。

- 生效时间：规则生效的起始时间和中止时间。格式为hhmm，例如“0803”，表示8时3分。
- 局域网IP地址：局域网中被控制的计算机的IP地址，为空表示对局域网中所有计算机进行控制。这也可以是一个IP地址段，例如192.168.1.123—192.168.1.185。
- （局域网）端口：局域网中被控制的计算机的服务端口，为空表示对该计算机所有服务端口进行控制。这也可以是一个端口段，例如1030—2000。
- 广域网IP地址：广域网中被控制的网站的IP地址，为空表示对整个广域网进行控制。这也可以是一个IP地址段，例如61.145.238.6-61.145.238.47。
- （广域网）端口：广域网中被控制的网站的服务端口，为空表示对该网站所有服务端口进行控制。这也可以是一个端口段，例如25-110。
- 协议：选择被控制的数据包所使用的协议。
- 通过：符合本条目所设置的规则的数据包是否可以通过路由器。
- 状态：本条过滤规则是否生效。
- 添加新条目：在过滤列表中添加新的过滤条目。
- 使所有条目生效：将该列表中所有过滤条目的状态设为“生效”。
- 使所有条目失效：将该列表中所有过滤条目的状态设为“失效”。
- 删除所有条目：删除当前已设的所有过滤条目。
- 移动：将某条记录移动到另一个位置，以达到不同的过滤优先级。（ID序号靠前则优先级较高）

举例说明：如果您希望局域网中IP地址为192.168.1.7的计算机全天不能收发邮件， IP地址为192.168.1.8的计算机在8：00-18：00时段内不能访问IP为



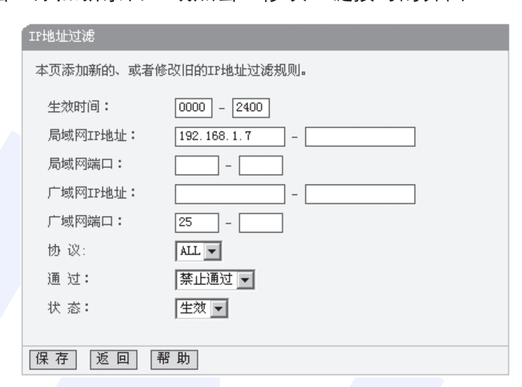




202.96.134.12的网站，对局域网中的其它计算机则不做任何限制，这时您需要作如下设置： 首先在“防火墙设置”中打开防火墙总开关，然后开启“IP地址过滤”，设置“缺省过滤规则”为“凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器”。然后，按照以下数据添加新的过滤条目：

| ID | 生效时间 | 局域网IP地址 | 端口 | 广域网IP地址 | 端口 | 协议 | 通过 | 状态 | 配置 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0000-2400 | 192.168.1.7 | - | - | 25 | ALL | 否 | 生效 | 编辑 删除 |
| 2 | 0000-2400 | 192.168.1.7 | - | - | 110 | ALL | 否 | 生效 | 编辑 删除 |
| 3 | 0800-1800 | 192.168.1.8 | - | 202.96.134.12 | - | ALL | 否 | 生效 | 编辑 删除 |

以下是您点击“添加新条目”或点击“修改”链接时的界面。




## 5.7.3 域名过滤

域名过滤

本页通过域名过滤来限制局域网中的计算机对某些网站的访问。

防火墙相关设置（如需更改，请到“安全设置”－“防火墙设置”）
防火墙功能： **开启**
域名过滤功能： **开启**

| ID | 生效时间 | 域 名 | 状 态 | 配 置 |
|---|---|---|---|---|
| 1 | 0000-2400 | www.xxyy.com.cn | 生效 | 编辑 删除 |
| 2 | 0000-2400 | www.aabbcc.com | 生效 | 编辑 删除 |
| 3 | 0800-1800 | .net | 生效 | 编辑 删除 |

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

本页显示已设的域名过滤列表。您可以利用按钮—“添加新条目”来增加新的

过滤规则；或者通过“修改”、“删除”链接来修改或删除旧的过滤规则。

- 生效时间：规则生效的起始时间和中止时间。格式为hhmm，例如“0803”，表示8时3分。
- 域名：您希望管理的域名。
- 状态：是否使本条过滤规则生效。
- 添加新条目：在过滤列表中添加新的过滤条目。
- 使所有条目生效：将该列表中所有过滤条目的状态设为“生效”。
- 使所有条目失效：将该列表中所有过滤条目的状态设为“失效”。
- 删除所有条目：删除当前已设的所有过滤条目。

举例说明：如果您希望全天禁止局域网中的计算机访问www.xxyy.com.cn、www.aabbcc.com和在8：00－18：00时段内禁止访问所有以“.net”结尾的网站，这时您需要指定如下的域名过滤表： 首先在“防火墙设置”中打开防火墙总开关，然后开启“域名过滤”。

| ID | 生效时间 | 域 名 | 状 态 | 配 置 |
|---|---|---|---|---|
| 1 | 0000-2400 | www.xxyy.com.cn | 生效 | 编辑 删除 |
| 2 | 0000-2400 | www.aabbcc.com | 生效 | 编辑 删除 |
| 3 | 0800-1800 | .net | 生效 | 编辑 删除 |

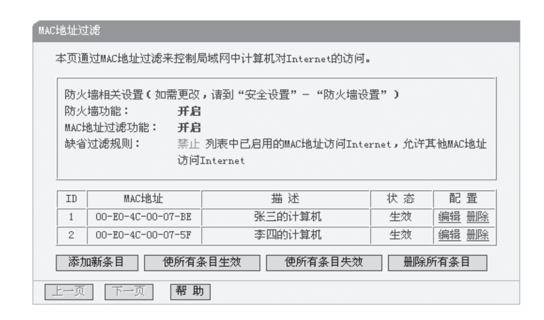
以下是您点击“添加新条目”或点击“修改”链接时的界面。








## 5.7.4 MAC地址过滤




本页显示已设的MAC地址过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“修改”、“删除”链接来修改或删除旧的过滤规则。

- MAC地址：您希望管理的计算机的MAC地址。
- 描述：对该计算机的适当描述。
- 状态：是否使本条过滤规则生效。
- 添加新条目：在过滤列表中添加新的过滤条目。
- 使所有条目生效：将该列表中所有过滤条目的状态设为“生效”。
- 使所有条目失效：将该列表中所有过滤条目的状态设为“失效”。
- 删除所有条目：删除当前已设的所有过滤条目。

举例说明：如果您不希望局域网中MAC地址为00-E0-4C-00-07-BE和00-E0-4C-00-07-5F的计算机访问Internet，而希望局域网中的其它计算机能访问Internet，这时您需要指定如下的MAC地址过滤表： 首先在“防火墙设置”中打开防火墙总开关，然后开启“MAC地址过滤”，设置“缺省过滤规则”为“禁止已设MAC地址列表中已启用的MAC地址访问Internet，允许其它MAC地址访问Internet”。然后，按照以下数据添加新的过滤条目：

| ID | MAC地址 | 描 述 | 状 态 | 配 置 |
|---|---|---|---|---|
| 1 | 00-E0-4C-00-07-BE | 张三的计算机 | 生效 | 编辑 删除 |
| 2 | 00-E0-4C-00-07-5F | 李四的计算机 | 生效 | 编辑 删除 |

以下是您点击“添加新条目”或点击“修改”链接时的界面。

MAC地址过滤

本页通过MAC地址过滤来控制局域网中计算机对Internet的访问。

MAC 地址： 00-E0-4C-00-07-BE

描 述： 张三的计算机

状 态： 生效

保 存 返 回 帮 助

### 5.7.5 远端WEB管理

远端WEB管理

本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。

注意： 1、路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口（例如改为88），则您必须用“IP地址:端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才能生效。
2、路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。

WEB管理端口： 80

远端WEB管理IP地址： 222.88.88.222

保 存 帮 助

本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。

- WEB管理端口：可以执行WEB管理的端口号。
- 远端WEB管理IP地址：广域网中可以执行远端WEB管理计算机的IP地址。



**注　意：**

1、 路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口（例如改为88），则您必须用“IP地址:端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才能生效。

2、 路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理，如果改为255.255.255.255，则WAN中所有主机都可以登录路由器执行远端WEB管理。

### 5.7.6 高级安全设置

高级安全选项

本页设置高级安全防范配置。只有当“DOS攻击防范”启用的时候，其后面的设置才能够生效。（注意：这里的“数据包统计时间间隔”与“系统工具”－“流量统计”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。）
另外：由于“DoS攻击防范”的部分功能是以相关数据包的统计为依据的，因此，如果“系统工具”－“流量统计”中的流量统计功能被关闭，那么将会导致这部分功能失效。同时该功能还受“防火墙设置”中的“开启防火墙”的影响。

数据包统计时间间隔：（5～60） 10 秒

DoS攻击防范： 不启用 启用

开启ICMP-FLOOD攻击过滤：

ICMP-FLOOD数据包阀值：（5～3600） 50 包/秒

开启UDP-FLOOD过滤：

UDP-FLOOD数据包阀值：（5～3600） 500 包/秒

开启TCP-SYN-FLOOD攻击过滤：

TCP-SYN-FLOOD数据包阀值：（5～3600） 50 包/秒

忽略来自WAN口的Ping：

禁止来自LAN口的Ping包通过路由器：

保 存 帮 助 DoS 被禁主机列表

- 数据包统计时间间隔：对当前这段时间里的数据进行统计，如果统计得到的某种数据包（例如UDP FLOOD）达到了指定的阈值，那么系统将认为UDP-FLOOD 攻击已经发生，如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包,从而达到防范攻击的目的。
- DoS攻击防范：这是开启以下所有防范措施的总开关，只有选择此项后，以下的几种防范措施才能生效。

- 开启ICMP-FLOOD攻击过滤：如果需要防范ICMP-FLOOD攻击，请选择此项。
- ICMP-FLOOD数据包阈值：当开启ICMP-FLOOD功能时，如果ICMP包到达这个指定的数目，防范措施则立即启动。
- 开启UDP-FLOOD攻击过滤：如果需要防范UDP-FLOOD，请选择此项。
- UDP-FLOOD数据包阈值：当开启UDP-FLOOD功能时，如果UDP包到达这个指定的数目，防范措施则立即启动。
- 开启TCP-SYN-FLOOD攻击过滤：如果需要防范TCP-SYN-FLOOD，请选择此项。
- TCP-SYN-FLOOD数据包阈值：当开启TCP-SYN-FLOOD功能时，如果TCP的SYNC包到达这个指定的数目，防范措施则立即启动。
- 忽略来自WAN口的Ping：当开启该功能后，广域网的计算机将不能Ping到本路由器。
- 禁止来自LAN口的Ping包通过路由器：当开启该功能后，局域网的计算机将不能Ping到广域网的计算机。
- DOS被禁主机列表： 点击该按钮，显示被禁主机列表，若希望被禁主机能够重新上网，则点击“删除”，如需释放所有被禁主机，点击图中的“清空”按钮。




## 5.8 路由功能

- 路由功能
  - 静态路由表







在“路由功能”菜单下面，只有“静态路由表”一个子项。单击该子项，您即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

### 5.8.1 静态路由表




本页设置路由器的静态路由功能，您可以利用按钮—“添加新条目”来增加新的路由条目；或者通过“编辑”、“删除”链接来修改或删除旧的路由条目。

- 目的IP地址：欲访问的主机的IP地址。
- 子网掩码：填入子网掩码，一般为255.255.255.0。
- 网关：数据包被发往的路由器或主机的IP地址。
- 状态：是否使本条目生效。
- 添加新条目：在路由列表中添加新的条目。
- 使所有条目生效：将该列表中所有条目的状态设为“生效”。
- 使所有条目失效：将该列表中所有条目的状态设为“失效”。
- 删除所有条目：删除当前已设的所有条目。

以下是您点击“添加新条目”或点击“编辑”链接时的界面。



## 5.9 动态DNS（DDNS）

### 5.9.1 花生壳DDNS




本页设置“花生壳”的DDNS参数。当连接状态显示成功后，互联网上的其它主机就可以通过域名方式对您的路由器或虚拟服务器进行访问。

- 服务商链接：点击链接访问服务商的网站，您可以进行注册和获得帮助。
- 服务提供者：提供DDNS的服务器。
- 用户名：在DDNS服务器上注册的用户名。
- 密 码：在DDNS服务器上注册的密码。
- 启用DDNS：选中则启用DDNS功能，否则关闭DDNS功能。
- 连接状态：当前与DDNS服务器的连接状态。
- 服务类型：当前的DDNS服务类型。
- 域名信息：当前从DDNS服务器获得的域名服务列表。

### 5.9.2 科迈DDNS







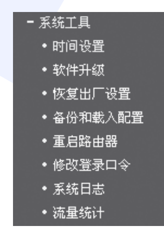

本页设置“科迈网”的DDNS参数。当连接状态显示成功之后，互联网上的其它主机就可以通过以域名的方式对您的路由器或虚拟服务器进行访问了。

- 服务提供者：提供DDNS的服务器。
- 域名信息：在DDNS服务器上已经注册的域名服务列表。
- 用户名：在DDNS服务器上注册的用户名
- 密 码：在DDNS服务器上注册的密码。
- 连接状态：当前与DDNS服务器的连接状态。

**注 意：**

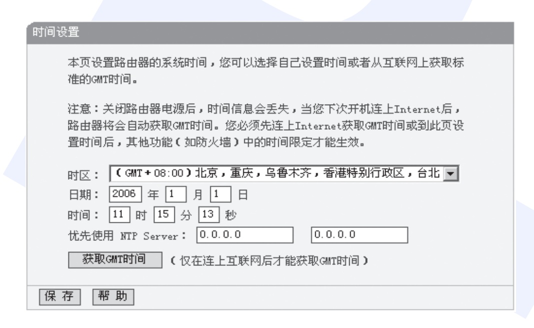
由于DDNS服务提供商所导致的DDNS功能失效与我司无关。

## 5.10 系统工具



在“系统工具”菜单下面，共有“时间设置”、“软件升级”、“恢复出厂设置”、“备份和载入配置”、“重启路由器”、“修改登录口令”、“系统日志”和“流量统计”八个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

### 5.10.1 时间设置




本页设置本路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的GMT时间。

系统时间设置步骤如下：首先请您先选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击“保存”完成系统时间的设置。

如果您已经连上了互联网，则您也可以直接单击“获取GMT时间”从互联网上获取标准的GMT时间。

 **注　意：**

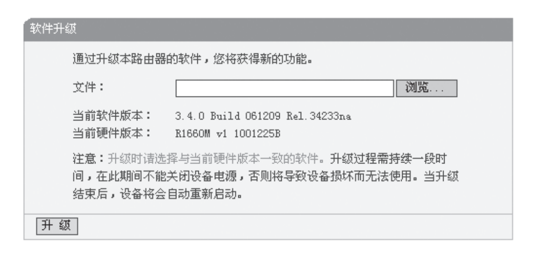
关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能（如防火墙）中的时间限定才能生效。







### 5.10.2 软件升级




通过升级本路由器的软件，您将获得新的功能。

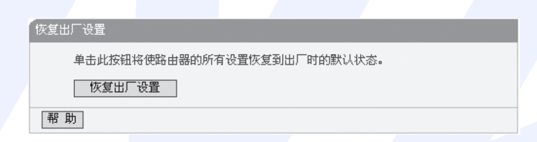
软件升级步骤：

1) 登录我们公司的网站(www.tp-link.com.cn)，下载最新版本的软件。
2) 在文件栏内填入已下载文件的全路径文件名，或用浏览按钮选择文件。
3) 单击“升级”进行软件升级。
4) 升级完成后，路由器将自动重启动

 **注　意：**

升级时请选择与当前硬件版本一致的软件。升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重新启动。

### 5.10.3 恢复出厂设置



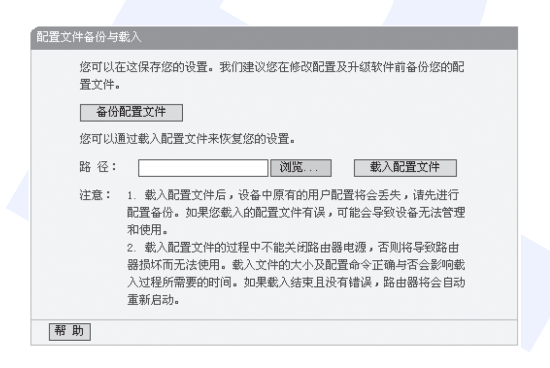

单击“恢复出厂设置”按钮将使路由器的所有设置恢复到出厂时的默认状态。其中：

- 默认的用户名为：admin
- 默认的密码为：admin

- 默认的IP地址为：192.168.1.1
- 默认的子网掩码为：255.255.255.0

恢复出厂设置后，路由器将自动重启动。

### 5.10.4 备份和载入配置




配置备份功能可以将您的设置以文件形式保存到您的电脑中，以备下次使用；配置载入功能是将先前保存的或已编辑好的配置重新装入。典型的用法是：

1) 升级软件或载入新配置文件前备份配置，以防止升级软件或载入新配置文件时操作有误，而丢失配置。
2) 为多台路由器配置相同设置：设置一台路由器，保存后，再载入其它的路由器中，以节省时间。

在备份和载入配置界面中：

- 备份配置文件：将设置以文件形式保存
- 路径：配置文件的全路径
- 浏览：选择配置文件
- 载入配置文件：装入先前保存的或已编辑好的配置





 **注 意：**

1) 载入配置文件后，设备中原有的用户配置将会丢失，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。
2) 载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，然后最好重启路由器。

在本例中，备份配置到：C:\Router\firmware\config.bin；然后，将其载入到另一台路由器中。

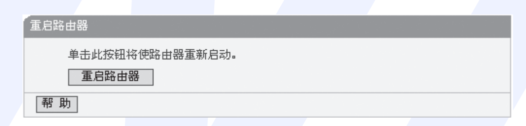
- 备份配置

系统工具>备份和载入配置，单击备份配置文件按钮，并按提示进行，将配置文件config.bin保存在以下文件夹中C: \Router\firmware。

- 载入配置

更换另一台路由器，系统工具>备份和载入配置，在“路径”文本框中输入以下内容，然后单击载入配置文件按钮：路径C:\Router\firmware\config.bin或点击浏览选择。

### 5.10.5 重启路由器




如果单击重启路由器按钮，路由器就会重新启动，您会见到如下界面：



## 5.10.6 修改登录口令



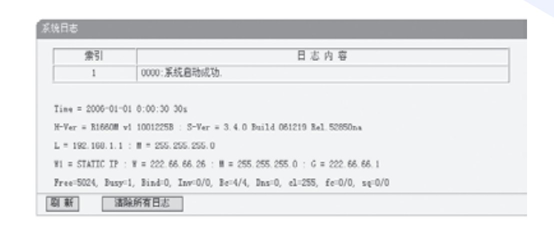

本页修改系统管理员的用户名及口令。

请您首先输入原来的用户名和口令，然后输入您希望使用的新用户名和口令，如果您原来的用户名和口令输入无误的话，单击“保存”即可成功修改用户名和口令。

 **注　意：**

出于安全考虑，我们强烈推荐您改变初始系统管理员用户名及密码。如果您忘了系统密码，请将路由器恢复到出厂设置（如何恢复请参考章节3.1.2）。

## 5.10.7 系统日志




该部分记录了路由器的系统日志，您可以通过查询日志了解路由器上所发生的系统事件。







## 5.10.8 流量统计

数据包统计时间间隔：该数值决定了统计当前流量的时间间隔。它与“安全设置”—“高级安全设置”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。

- IP地址：被统计主机的IP地址。
- 总流量：数据包数— 路由器总的收、发数据的包的个数。
  - 字节数：路由器总的收、发数据的字节数。
- 当前流量：数据包数— 路由器当前 10 秒钟收、发数据的包的个数。
  - 字节数：路由器当前 10 秒钟收、发数据的字节数。
  - ICMP Tx：路由器当前 10 秒钟发送到广域网的ICMP包的个数。
  - UDP Tx：路由器当前 10 秒钟发送到广域网的UDP包的个数。
  - TCP SYN Tx：路由器当前 10 秒钟发送到广域网的TCP SYN 包的个数。
- 开启/关闭流量统计：如无需流量统计，可通过按钮进行关闭，可提高路由器的数据处理能力。

 **注　意：**

由于“安全设置”-“高级安全设置”中“DoS攻击防范”的部分功能是以相关数据包的统计为依据的，因此，如果流量统计功能被关闭，那么将会导致这部分功能失效。

# 附录A 常见问题解答

1、ADSL 用户如何设置上网?

1) 首先，将ADSL modem设置为桥模式（1483桥模式）。

2) 用网线将路由器的WAN口与ADSL modem相连，电话线连ADSL modem的Line口。

3) 进入管理界面，选择菜单“网络参数”下的“WAN口设置”，在右边主窗口中，“WAN口连接类型”选择“PPPoE”，输入“上网账号”及“上网口令”，点击连接按钮即可。

4) 如果是包月上网的用户，可以选择“自动连接”的连接模式；如果是非包月用户，可以选择“按需连接”或者“手动连接”，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

2、LAN接入的用户如何设置上网?

1) 进入管理界面，选择菜单“网络参数”下的“WAN口设置”，在右边主窗口中，“WAN口连接类型”选择“动态IP”，点击“保存”按钮即可。

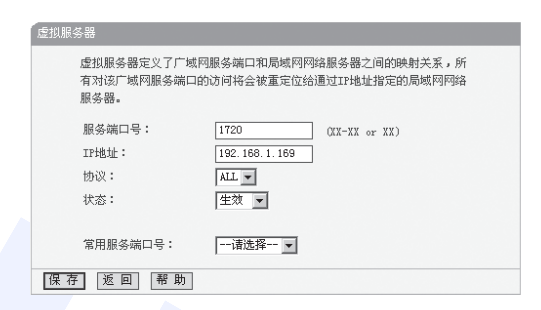
2) 在某些网络服务商绑定了用户计算机网卡MAC地址的情况下，需要对路由器进行MAC地址克隆操作，将路由器的WAN口MAC地址设置为被绑定的网卡MAC地址。选择菜单“网络参数”下的“MAC地址克隆”，在右边主窗口中点击“克隆MAC地址”按钮，然后按“保存”按钮，待路由器重启动后生效。

3、怎样使用NetMeeting聊天?

1) 如果是主动发起NetMeeting连接，则不需要任何配置，直接在NetMeeting界面中输入对方的IP地址，即可进行NetMeeting呼叫。

2) 如果希望能接收来自对方NetMeeting呼叫，则需设置虚拟服务器或DMZ主机。

3) 设置虚拟服务器方法：进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“1720”，这是NetMeeting的连接端口，“IP地址”栏填入您计算机的IP地址(假设IP地址是192.168.1.169)，再在状态栏选择“生效”，点击“保存”按钮即可。如图：




对方呼叫您时输入您路由器WAN口地址。

4) 设置DMZ主机方法：进入管理界面，选择菜单“转发规则”下的“DMZ主机”，在“DMZ主机IP地址”栏填入您计算机的IP地址(假设IP地址是192.168.1.169)，再将“启用”选择框选中，点击“保存”按钮即可。如图：

DMZ主机

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。
（注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。）

DMZ 状态： 启用 不启用

DMZ 主机IP地址： 192.168.1.169

保 存 帮 助

4、怎样在局域网构建Web服务器?

1) 在局域网构建服务器，只需要按问题3的第三点设置虚拟服务器即可。

2) 若构建Web服务器时，Web的服务端口与路由器Web管理界面的缺省端口相同，都是80，就会引起冲突。解决办法是修改路由器Web管理界面的端口。

3) 进入管理界面，选择菜单“系统工具”下的“远端Web管理”，在右边主窗口中，“Web管理端口”栏输入80以外的值，如88。点击保存并重启路由器。如图：

远端WEB管理

本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。

注意： 1、路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口（例如改为88），则您必须用“IP地址:端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才能生效。
2、路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。

WEB管理端口： 88
远端WEB管理IP地址： 0.0.0.0

保 存 帮 助

4) 再次进入管理界面，需要在浏览器的地址栏输入：http://192.168.1.1:88 才能进入。

5) 进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“80”，这是Web服务器的连接端口，“IP地址”栏填入Web服务器的IP地址(假设您的Web服务器的IP地址是192.168.1.188)，再在状态栏选择“生效”，点击“保存”按钮即可。如图：

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号： 80 (XX-XX or XX)
IP地址： 192.168.1.188
协议： ALL
状态： 生效

常用服务端口号： --请选择--

保 存 返 回 帮 助



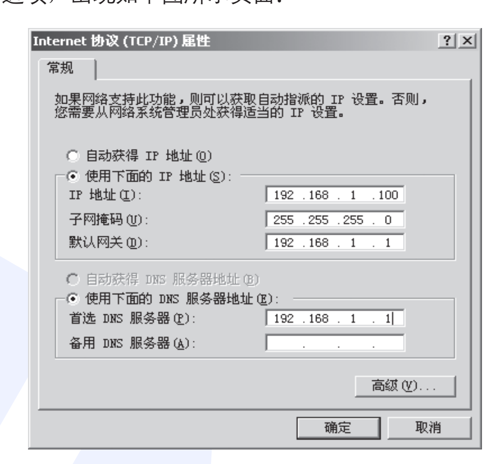




# 附录B TCP/IP的详细配置

在这一节中我们将详细介绍TCP/IP的配置(本部分内容以Win 2000 为例):

1、 打开“控制面板”中的“网络连接”，右键点击“本地连接”图标，单击“属性”选项，出现如下图所示页面：




2、 双击“Internet 协议”（TCP/IP），出现如下图所示页面：

Internet 协议 (TCP/IP) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I):
子网掩码(U):
默认网关(D):

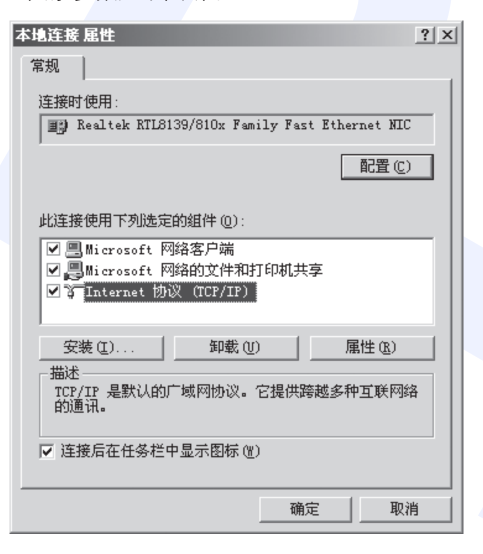
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P):
备用 DNS 服务器(A):

高级(V)...

确定 取消

3、 如果您希望自动从路由器获得IP地址，请选择自动获得IP地址和自动获得DNS服务器地址，点击确定后设置生效。

如果您希望拥有固定的IP地址，请选择使用下面的IP地址和使用下面的DNS服务器地址，然后手动设置网络参数，其中IP地址为192.168.1.2－192.168.1.254范围内的任意值，其余参数如下图所示：










# 附录C 术语解释

- DNS (Domain Name Server)：域名解析服务器。Internet上的计算机是通过IP地址来定位的，给出一个IP地址，就可以找到Internet上的某台主机。通过域名并不能直接找到要访问的主机，中间要加一个从域名查找IP地址的过程，这个过程就是域名解析。负责将域名解析成为IP地址的服务器，叫做域名解析服务器（Domain Name Server,即DNS）。
- DDNS (Dynamic Domain Name Server)：动态域名服务。将用户的动态IP地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态IP地址传送给位于服务商主机上的服务器程序，服务项目器程序负责提供DNS服务并实现动态域名解析。
- DHCP (Dynamic Host Configuration Protocol)：动态主机配置协议。DHCP服务器的功能是给网络中设置为自动获得IP地址的电脑分配网络参数。
- DMZ (Demilitarized Zone)：为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，有效保护内部网络。一般情况下，路由器屏蔽了内网的网络情况，如果一个连接是由外网主动向内网内中的某台主机发起的，那么由于路由器的存在，这样的连接是不能够建立的。路由器将这些连接请求都丢弃掉。而当我们把某一台内网主机设置成DMZ后，路由器不会只是简单的把这些数据包简单的丢弃，而是把外网对DMZ主机的请求转发给DMZ主机。这样，DMZ主机就充分的暴露给了外网，使得由外网发起的连接也可以成功实现。而内网中的其他主机仍然处在路由器的保护之下。
- GMT (Greenwich Mean Time)：格林尼治标准时间。
- ISP (Internet Service Provider)：网络服务提供商。

- LAN (Local Area Network)：局域网。
- L2TP (Layer 2 Tunneling Protocol)：第二层隧道协议，用于拨号上网。
- MAC (Media Access Control)：介质访问控制。MAC地址是识别LAN（局域网）节点的标识。网卡的物理地址通常是由网卡生产厂家烧入网卡的EPROM（一种闪存芯片，通常可以通过程序擦写），它存储的是传输数据时真正赖以标识发出数据的主机和接收数据的主机的地址。
- MTU (Maximum Transmission Unit)：网络上传送的最大数据包。MTU的单位是字节。 大部分网络设备的MTU都是1500。如果本机的MTU比网关的MTU大，大的数据包就会被拆开来传送，这样会产生很多数据包碎片，增加丢包率，降低网络速度。把本机的MTU设成比网关的MTU小或相同，就可以减少丢包。
- PPPoE (Point-to-Point Protocol over Ethernet)：通过以太网的点对点协议，用于拨号上网。
- PPTP (Point-to-Point Tunneling Protocol)：点对点隧道协议，用于拨号上网。
- UPnP (Universal Plug-and-Play)：通用即插即用。它的目的是让电脑可以自动发现前端的NAT路由器设备，并自动根据软件的需要在路由器上设置打开相应的端口。用户不需要手工去添加端口转发，这在一些端口不固定的应用上更加方便，比如MSN聊天工具的语音功能所使用的端口就是不固定，之前只能使用DMZ功能来转发，但是这样一个路由器下面最多就只有一个电脑可以使用MSN语音。UPnP则不同，每一台电脑只自动转发一个端口，所以可以多人同时语音聊天。
- VPN (Virtual Private Network)：虚拟专用网。这是建立在实际网络上的一种功能性网络。在VPN网络中，位于公共网络两端的网络在公共网络上传输





信息时，其信息都是经过安全处理的，可以保证数据的完整性、真实性和私有性。

- VPN Pass-through：指设备能够识别由内网主机发起的，到外网VPN SERVER的VPN类型的数据。由于VPN数据是经过加密处理的，设备若不具备此类型数据的识别能力，可能将VPN数据丢弃，导致VPN建立失败。
- WAN (Wide Area Network)：广域网，也就是我们通常说的Internet网。